

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)A RED IPHONE WITH RED CASE, LOCATED AT U.S.  
SECRET SERVICE, 200 W. SECOND STREET,  
SUITE 811, DAYTON, OHIO 45402

Case No.

3:20MJ141

APPLICATION FOR A SEARCH WARRANT BY TELEPHONE OR OTHER RELIABLE  
ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

SEE ATTACHMENT C

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature

SA TREVOR CANFIELD, U.S. SECRET SERVICE

Printed name and title

Sworn to before me and signed in my presence via facetime.

Date: 3-17-20City and state: DAYTON, OHIO
  
 Judge's signature

SHARON L. OVINGTON U.S. MAGISTRATE JUDGE

Printed name and title

**AFFIDAVIT**

I, Trevor Canfield, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application made pursuant to Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of certain previously seized property—to wit: electronic devices, all of which are currently possessed, maintained and securely stored by the United States Secret Service (USSS). This application specifically seeks authority to extract from said devices electronically stored information which is more specifically described in Attachment B.

2. I am currently a Special Agent (SA) with the USSS, and have been so employed since September 2017. I have received extensive training in conducting criminal investigations involving certain offenses set forth in Title 18 of the United States Code. I am currently assigned to the Dayton Resident Office. I have previously participated in a wide variety of financial-crime investigations, to include: Credit/Debit/Gift Card Fraud, Identity Theft, Aggravated Identity Theft, Access Device Fraud, Fraud in Connection with Computers, Bank Fraud, Wire Fraud, and Conspiracy, in violation of Title 18, United States Code, §§ 1028, 1028A, 1029, 1030, 1343, 1344, 371, and 1349 respectively. I have attended and completed multiple law enforcement training courses conducted at: the Department of Criminal Justice Training Academy (DOCJT) located in Richmond, KY; the Federal Law Enforcement Training Center (FLETC) located in Glynco, Georgia; and the James J. Rowley United States Secret Service Training Center (JJRTC) located in Laurel, Maryland. Prior to becoming a SA with the USSS, I served as a Patrol Deputy and a member of the Special Weapons and Tactics (SWAT) team with the Boone County (KY) Sheriff's Office located in Burlington, KY.

3. This affidavit is intended to only set forth sufficient facts to establish the necessary probable cause to justify the issuance of the requested search warrants. It does not

contain all the facts presently known by your Affiant relating to the subject investigation. The facts set forth in this affidavit are based upon your Affiant's personal knowledge and training, coupled with other information provided to him by various law enforcement officials familiar with subject investigation, together with a review of various law enforcement reports of investigation generated during the course of subject investigation.

**IDENTIFICATION OF THE DEVICES TO BE EXAMINED**

4. The property sought to be searched consists of: a WHITE IPHONE 10 hereinafter referred to as Device #1; an unknown version of an IPHONE (damaged) inside of BLACK CASE hereinafter referred to as Device #2; an ACER CHROME LAPTOP COMPUTER, Serial # NXGV2AA002927094067600, Model# N17Q8, SNID: 92703789476 hereinafter referred to as Device #3; a BLACK LG CELL PHONE WITH CRACKED SCREEN hereinafter referred to as Device #4; an IPHONE7 WITH BLACK CASE hereinafter referred to as Device #5; a RED IPHONE WITH RED CASE hereinafter referred to as Device #6; a SILVER IPHONE WITH BLACK CASE AND RED COVER IMEI: 354387064785382, MODEL: A1522, FCC ID: BCG-E2817A hereinafter referred to as Device #7; and a BLACK AND SILVER IPAD, MODEL: A2200, SERIAL # GG7ZCGG0MDG1 hereinafter referred to as Device #8.

5. All said Devices are presently stored and maintained in a secure evidence locker located at the U.S. Secret Service Offices located at 200 West Second St., Ste. #811, Dayton, OH 45402. They remain in the same state and condition as when they were first transferred to the USSS' custody from the various local law enforcement agencies who originally seized them.

6. The applied-for warrants seek authorization to forensically exam each of the aforesaid Devices for the express purpose of identifying and reviewing certain electronically stored data deemed relevant to the subject investigation, more particularly described in Attachment B.



**PROBABLE CAUSE**

7. On or about July 19, 2019, the USSS Dayton Resident Office opened a formal investigation into a Dayton, Ohio based criminal conspiracy which has been illicitly using stolen credit card account information to purchase large amounts of gas from local gas stations and convenient stores. This criminal conspiracy dates back to at least the late-2018 time frame. The law enforcement agencies involved in subject investigation include: the Clark County Sheriff's Office, the Montgomery County Sheriff's Office, the Englewood Police Department, the Huber Heights Police Department, the Dayton Police Department, the Harrison Township Police Department, the Riverside Police Department, the Kettering Police Department, and the New Lebanon Police Department.

8. Subject investigation has established that members of a criminal conspiracy purchased bulk amounts of stolen credit card account numbers from encrypted internet web sites located on the so-called "Dark Web." These stolen credit card account numbers were thereafter re-encoded onto credit/debit/gift cards for later illicit use in purchasing large amounts of gas at local area gas stations and convenient stores. Members of the conspiracy posted notices on designated *Facebook* pages to advertise to prospective "customers" as to the upcoming dates, times, and locations that illicit gas sales, i.e., "fill-ups" would be available. The specific *modus operandi* employed by the conspiracy consisted of collecting \$20.00 in cash from "customers" in return for a full tank of gas dispensed by one of the conspiracy's "gas pump operators" who would gain access to the gas pump through the fraudulent use of a credit/debit/gift cards previously re-encoded with a stolen credit card account number. The "gas pump operator" would refrain from returning the gas nozzle to the gas pump between serving the multiple "customers", who would typically be lined up at the pumps awaiting gas fill-ups. This process would avoid activating the gas pump's automatic shut off mechanism.



**FACTS RELEVANT TO DEVICES #1 AND #2**

9. At approximately 1355 hours on November 4, 2019, Kettering Police Department (KPD) Officers Maloney and Woolf were dispatched to a United Dairy Farmer's (UDF) Store located at 2200 E. Dorothy Lane, Kettering, OH 45420. Store employees, had reported observing a suspicious yellow, Chevrolet, Monte Carlo, believed to be involved in a fraudulent gas fill-up scheme. Earlier that day, these same two store employees had filed a similar report with KPD Officer Stewart concerning this same vehicle. The driver the said yellow Chevrolet, Monte Carlo had then been observed swiping multiple cards at the store's gas pump in order to purchase gas for multiple other vehicles.

10. Officer Woolf subsequently located and stopped the suspect vehicle near the intersection of Woodman and Rainbow Drives. The female driver, who was identified to be Alijia Netelai Irene Whitner, was cited for driving while under suspension. The male passenger located inside the suspect vehicle was identified to be **DARRELL TOSHE WHITE, JR.** KPD determined that **WHITE** then had an active arrest warrant. In accordance with established KPD policy, the vehicle was impounded, inventory searched and ordered towed from the scene. During the course of said inventory search, multiple credit cards, debit cards, and gift cards were found inside the vehicle's glove box. Cards were also found inside **WHITE's** wallet. KPD Officers also located and seized two cell phones that were found in **WHITE's** possession, to wit: a WHITE IPHONE 10 hereinafter referred to as Device #1; and unknown version of an IPHONE (damaged) inside of BLACK CASE hereinafter referred to as Device #2.

11. Law enforcement authorities attempted to interview **WHITE**, however he invoked his 5<sup>th</sup> Amendment right to remain silent.

12. Your Affiant subsequently collaborated with KPD to examine and scan the various seized cards. This examination determined that 12 of the 14 seized cards had in-fact been re-encoded with stolen credit card information.

13. On December 9, 2019, your Affiant took custody of Devices #1 and #2 on behalf of the USSS. Since said date, Devices #1 and #2 have remained in the secure custody of the USSS.

**FACTS RELEVANT TO DEVICES #3 AND #4**

14. At approximately 2137 hours on December 18, 2019, Dayton Police Department (DPD) Officers Eck and Lane were dispatched to 819 Princeton Dr. due to a report of gun shots being discharged as detected by DPD's new computerized "Shot Spotter" tracking system. This system determined that gun shots had been fired at or near the rear of an apartment building located at 1124 Salem Avenue.

15. Upon arriving on-scene, the Officers observed that a second floor apartment balcony door was left ajar. This was considered particularly unusual due to the fact the outdoor temperature was then determined to be approximately 18° F.

16. Officers additionally observed the presence of multiple spent 9 mm gun shell casings found laying on the back steps of the apartment building leading up to the common entrance hallways. A resident of the apartment building advised the Officers that an unusually large number of individuals were commonly observed coming and going from Apartment #8.

17. Officers next proceeded up the stairway to the second floor where they made contact with a resident of Apartment #7. This resident advised the Officers that he had heard arguing and shouting originating from inside of Apartment #8. He additionally reported hearing gunshots being fired from the rear of the apartment building. He further advised having made several previous complaints to DPD about the residents/guests of Apartment #8. He advised Officers that the occupants of that Apartment #8 have been nothing but trouble since they first moved in. He finally stated that it was not unusual to observe various individuals enter and depart this apartment carrying guns.

18. Officers then attempted to make contact with the occupants of Apartment #8. They knocked on the apartment door, but received no response. Officers then went to a second entrance door for said apartment and knocked again. That particular door swung open. Officers proceeded to loudly announce themselves multiple times. Finally someone from inside the apartment yelled back that they were home. Officers thereupon heard frantic rustling noises originating from the living room area of the apartment. The Officers could not visibly observe the individual who had previously responded from inside the apartment. Based upon a concern that this person could be: in distress, possibly connected with the gun shots, or otherwise engaged in some other suspicious or criminal activity; the Officers entered the apartment to further investigate the situation. At this point, an individual, (later identified to be Kristofer St. Jules) appeared from inside the apartment. St. Jules was observed to be sweating profusely and wearing clothes that appeared to be in a general state of disarray. St. Jules indicated to the Officers that he had been sleeping on the couch. At this point, the Officers observed the presence of what appeared to be two live ammunition rounds next to St. Jules. These rounds appeared to be similar to the spent shell casings the Officers previously observed outside of the apartment building. Due to the original nature of the reported "complaint," coupled with St. Jules' suspicious/unusual behavior and appearance, and the observed presence and location of the two live rounds, the Officers decided to perform a cursory officer security sweep of the area immediately surrounding the sofa area that St. Jules had just occupied. The purpose of this security sweep was to determine the presence of any firearms or other weapons that could pose a danger to the officers. As result of this security sweep, a small handgun was found tucked into one of the sofa cushions. Officers immediately secured the weapon and placed St. Jules in handcuffs. The seized handgun was observed to not have a magazine, and the chamber was empty. A further check of the sofa area located the missing gun magazine with two additional live rounds.



19. Upon observing the Officers retrieve the firearm from the sofa, St. Jules blurted out: “that ain’t mine.” At that point, Officers also observed a loaded Glock high capacity magazine sticking out from the top of a work boot adjacent to the sofa. This magazine was determined to contain 21 live rounds. Officers also observed in plain view, located on the living room fireplace mantle, two large stacks of gift cards, next to an ACER CHROME LAPTOP COMPUTER, Serial # NXGV2AA002927094067600, Model# N17Q8, SNID: 92703789476 (hereinafter referred to as Device #3). Adjacent to this computer was a small back pack which contained a partially visible swipe card reader. A variety of drug related paraphernalia was also visible in plain view on the kitchen counter, to wit: a plastic baggie containing an unknown white powdery substance, and hypodermic needles. These two items appeared to be illegal drugs and drug paraphernalia respectively. St. Jules was thereafter taken into custody and transported to the DPD Public Safety Building for interviewing.

20. Prior to questioning, St. Jules was advised of his Fifth Amendment *Miranda* Rights. He waived his rights and agreed to be interviewed.

21. St. Jules stated that he house sitting for his cousin **TROY THOMAS** who was apparently out of town for three days. His cousin’s dog required looking after, and his apartment had previously been broken into. St. Jules further stated that his cousin promised to pay him \$50-\$100 for watching his apartment. St. Jules further stated that **THOMAS** is 21 years of age and has a girlfriend named Casey. He further stated that **THOMAS** does not have a criminal record or a job. St. Jules stated that the only personal property left in the apartment that was his was a pair of *AirMax* sneakers. St. Jules advised investigators that he is currently on probation. He reiterated that he had nothing to do with the firearm, gift cards, computer or drugs found inside of the apartment. St. Jules further stated that he believes **THOMAS’** girlfriend drives a black Nissan Altima. He further stated that he was asleep inside the apartment when he was awakened by the sound of gunshots.

22. St. Jules further stated that when he first arrived at his cousin's apartment, he noticed two stacks of gift cards on the mantle. He inquired of his cousin why he had them. **THOMAS** reportedly responded: "it's Christmas time." St. Jules further stated that he was aware of the existence of a so-called "\$20 Gas Fill-Up Scheme." He stated that it has been going around, and it's big in the city. St. Jules further stated **THOMAS** was expected to return back to his apartment in three days.

23. St. Jules advised that the first time he remembers learning about a so-called "Gas Fill-Up Scheme" during the summer of 2019. He further stated that he remembers being at a local Shell Gas Station when he observed a guy standing at the gas pumps with a gas pump nozzle in his hand which he never returned to the pump. He stated that this individual would continue pumping gas for various individuals collecting \$20 dollars from each individual prior to filling up their respective gas tanks. He further stated that on that occasion he observed about 15 cars lined up to receive gas from this person. He remembers actually getting into an argument with one of the guys orchestrating the fraud scheme because he refused to let him use the gas pump to fill up his own gas tank. St. Jules further advised that while he was arguing with this particular individual, the store's gas attendant switched off the gas pumps. As a result, all of the participating "customers" and criminal suspects dispersed from the area.

24. Your Affiant confiscated St. Jules' cell phone, to wit: a BLACK LG CELL PHONE WITH CRACKED SCREEN (hereinafter referred to as Device #4) due to the fact he was found in a premises that DPD had previously identified as a suspect drug stash house. At the time of St. Jules' apprehension, he was located in a premises where a laptop computer, re-encoded credit cards, a swipe card reader and handgun were located. Based upon your Affiant's knowledge of subject fraud scheme there appeared a probable cause to believe relevant evidence may exist on said cell phone.

25. Investigators displayed various photos for St. Jules to review. He positively identified a person previously known to law enforcement authorities as **TYSON THOMAS**.

26. The next day, on December 19, 2019, St. Jules left a voice message on Detective Delaney's answering machine advising that he had spoken to his cousin **TROY THOMAS** about the previous day's incident and the laptop computer left in his apartment. St. Jules stated that **TROY THOMAS** advised that the computer along with the gift cards belong to **TYSON THOMAS**, who left them the last time he was at the apartment. St. Jules indicated that neither he nor his cousin had anything to do with anything else, and to simply leave them alone.

#### **FACTS RELEVANT TO DEVICE #5**

27. On August 27, 2019, Harrison Township Police Department (HTPD) Officer Gebhart was dispatched to a Sunoco Gas Station located at 2001 Needmore Road in Harrison Township, OH 45414 in response to a stolen credit card complaint. The store employee claimed that a suspect was using a stolen credit card to purchase gas.

28. Upon arriving on-scene, Officer Gebhart observed an individual pumping gas into a Black Audi SUV. This individual was later identified to be **RAESHON BATTLE**. An unidentified male was observed occupying the driver's seat of said vehicle. Officer Gebhart asked **BATTLE** whether he had used a credit card to pay for his gas. **BATTLE** responded that he paid cash. Officer Gebhart next inquired whether he had pre-paid for the gas. **BATTLE** responded: "I'm about to pay for it." Officer Gebhart requested to see **BATTLE**'s identification. **BATTLE** stated he did not have a driver's license. At that point, **BATTLE** attempted to flee the scene on foot. Officer Gebhart gave chase and ultimately caught him. **BATTLE** shouted: "I'm sorry!" and proceeded to put his hands in the air. **BATTLE** was handcuffed, detained, "patted down" and placed in the back seat of Officer Gebhart's police cruiser. Thirty (30) gift cards from various businesses; and one (1) MasterCard debit card that had "Employee" embossed on it were found on **BATTLE**'s person. **BATTLE** was subsequently released, however the gift cards



were confiscated and turned over to the HTPD Detective Section for further investigation. It was later determined that the confiscated gift cards were re-encoded with stolen credit card information.

29. On October 26, 2019, Officers from KPD were dispatched to a UDF Store located at 2200 E. Dorothy Lane., Kettering, OH following a report of an on-going active fraudulent gas fill-ups. Upon arriving on-scene, a suspect vehicle was observed attempting to depart the scene. KPD Officers motioned the driver of said vehicle, later identified to be **DASHAUN T.D. STEWART-RAINEY**, to stop. **STEWART-RAINEY** complied with this police directive.

30. On the said date, a second suspect, later identified to be **RAESHON BATTLE**, was observed entering a vehicle parked at the same UDF Store. KPD Officers approached **BATTLE** and questioned why he was at the gas station. He responded that he was there to pay **STEWART-RAINEY** some money he owed him.

31. **BATTLE** provided the KPD Officers verbal consent to examine the contents of his wallet, and search his vehicle. The Officers failed to locate any embossed credit cards that matched the gas pump transaction receipts found inside of **BATTLE's** wallet or vehicle. Officers further observed the front license plate of **BATTLE's** vehicle lying on the front passenger seat. Officers also observed an unusually large amount of U.S. Currency located inside of the vehicle. **BATTLE** was allowed to depart the scene.

32. KPD Officers approached and interviewed **STEWART-RAINEY** regarding this incident. **STEWART-RAINEY** claimed he was simply getting gas. **STEWART-RAINEY** further stated that **BATTLE** inserted a credit card into the gas pump to pay for his gas. **STEWART-RAINEY** verbally consented to a search of both his wallet and his vehicle. **STEWART-RAINEY** was found to be in possession of multiple credit cards. Each of the credit cards were embossed with his name. **STEWART-RAINEY** was released and allowed to depart the scene.

33. On October 29, 2019, KPD officers responded to the said UDF Store to collect relevant gas receipts and store surveillance video as evidence.

34. On December 6, 2019, KPD Officers responded to a Shell Gas Station located at 5001 Bigger Rd., Kettering, OH in connection with a suspected gas fill-up scheme. A store employee reported to law enforcement authorities the presence of a gray Chevrolet vehicle at one of the store's gas pumps involved with the suspected fraudulent purchase of gas.

35. After KPD Officers responded to the Shell Gas Station, they made contact with the driver of the said gray Chevrolet vehicle. The driver was identified to be **RAESHON BATTLE**. **BATTLE** consented to a search of his person. As a result of this search, Officers found \$657.00 in U.S. Currency and 14 re-encoded gift cards. An IPHONE7 WITH BLACK CASE (hereinafter referred to as Device #5) was found on the front driver's seat of his vehicle.

36. At this same time, KPD Officers also made contact with another suspect identified as "Frank Smith." Smith stated that he was at the gas station to meet a "Shawn" for gas. Smith advised that he had used his cell phone to look up "Shawn's" phone number. Smith agreed to then call "Shawn's" telephone number. After punching in "Shawn's" telephone number, **BATTLE's** cell phone started ringing, and Smith's number appeared on the screen indicating he was the source of the incoming call.

37. In accordance with established KPD policy, Battle's vehicle was impounded, inventory searched and ordered towed from the scene. During the course of the inventory search, Officers located 20 re-encoded gift cards and two (2) white oval pills with "227" imprinted on them. When **BATTLE** was questioned about the gift cards, he stated that he sells and purchases re-encoded gift cards. **RAESHON BATTLE** was arrested and charged with Receiving Stolen Property in violation of O.R.C. § 2913.51.

38. On December 10, 2019, KPD Det. Jim Bodner, transferred custody of Device #5 to the USSS.

**FACTS RELEVANT TO DEVICES #6, #7 AND #8**

39. On September 20, 2019, Det. O'Connell of Montgomery Co. Sheriff's Office (MCSO), was conducting surveillance at a Marathon Gas Station located at 3905 N. Main Street, Harrison Twp., OH 45405 in reference multiple reported armed robberies occurring on the same date. Det. O'Connell then observed a black male, later identified to be **TYSON THOMAS** pumping gas into three (3) separate vehicles. Det. O'Connell further observed various vehicles pull up to pump #4, the driver of said vehicle then handed **THOMAS** cash. **THOMAS** would then fill up the respective cars with gas. **THOMAS** would place the gas pump handle on the ground between servicing the respective vehicles. As such, the gas pump's automatic shut off would not activate between servicing the respective cars.

40. **THOMAS** was thereafter observed getting into the back seat of a parked tan/gold Buick automobile. **THOMAS** was subsequently observed approaching a two-tone tan and brown Ford Crown Victoria automobile then parked at pump #3. Det. O'Connell observed **THOMAS** approach this car and speak with the driver through the passenger window. The said Ford Crown Victoria then departed the area. Det. O'Connell requested Dep. Wright to make contact with the driver and attempt to make further inquiries. Dep. Wright was able to make subsequent contact with the driver who was identified as "D.O." The driver provided law enforcement authorities with a written statement indicating a black male matching **THOMAS'** description had approached his car at the gas station and inquired of him whether he wanted to buy some gas. The driver said he did, and proceeded to give **THOMAS** \$10.00. **THOMAS** thereafter filled up "D.O's" gas tank.

41. Continuing on this date, Det. O'Connell and Dep. O'Brien while in a marked MCSO police cruiser, approached the rear of the said parked Buick. As the Officers approached the vehicle, **THOMAS** was observed making furtive movements toward the floor board. Det. O'Connell performed a furtive movement search of the floor board area. Three (3) crumpled up



\$20.00 bills were observed to be laying on the floor board area. They were thereafter seized. **THOMAS** was thereafter detained and placed in the back of the MCSO cruiser.

42. Continuing on this date, Det. O'Connell entered the said gas station and notified the store owner of the incident. Another store employee advised Det. O'Connell that a black VW Jetta operated by a black male with dread locks had recently been observed pumping gas in the same fraudulent manner. The store employee ordered him to leave. Det. O'Connell then collected the receipts from gas pumps #3 and #4 and requested access to the store's surveillance video.

43. Continuing on this date, **THOMAS** was transported to the MCSO HQ for interview. Following advisement of his 5<sup>th</sup> Amendment *Miranda* right, **THOMAS** agreed to be interviewed. He advised that he had recently been released from prison due to a previous drug conviction. He indicated he has a friend, named "**TONE**" who turned him onto a "gas fill-up" fraud scheme. He described "**TONE**" as a black male with shoulder length dread locks who drives a VW Jetta. **THOMAS** refused to reveal "**TONE's**" actual name or provide any additional information. He further stated that "**TONE**" had recently come by and swiped a card and filled the Buick up with gas. **THOMAS** then proceeded to fill-up another individual's gas tank for cash. He further stated that he had done this three times prior to being detained by law enforcement authorities.

44. On October 20, 2019, Riverside PD (RPD) Officers Ruchel and Sullivan were dispatched to Sammy's Gas Station located at 1290 Woodman Dr., Dayton, OH 45432 in reference to a possible gas fraud/theft incident in progress. The RPD Police Dispatcher advised the Officers that two unknown black males were reportedly using the same credit card at several gas pumps to fill-up multiple vehicles simultaneously. The store employee stated that the suspects made at least 12 fraudulent transactions, totaling \$1,136.59 in value. The store employee further stated that that one of the suspects was described as a black male wearing white

warm up pants and a Chicago Bears football jersey bearing #34. This particular suspect also had a beard and was wearing black tennis shoes with white soles. The store employee further described the second suspect as a black male wearing a black warm up suit. Both suspects were believed to be between the ages of 20-30 years old. The RPD Police Dispatcher advised that the two suspects were last seen walking on foot towards apartments located at 4290 Linden Ave.

45. On said date, two suspicious vehicles were observed leaving said gas station. The first vehicle was described as a Beige Chevy Tahoe bearing OH registration of HNG6773. Law enforcement determined that this vehicle was then operated by a **ANTHONY L. COOPER-KING**. The second vehicle was a White Chevy Silverado bearing OH registration of HPQ3405. Law enforcement determined that this vehicle was then operated by a **BRITTANY D. MUSTARD**. Both vehicles were subsequently stopped by law enforcement authorities and both drivers interviewed. **KING** denied having any involvement in any fraudulent gas purchase scheme, and further denied knowing any suspects that may have been involved. **KING** is currently on parole for aggravated robbery and has several theft related convictions in his criminal history. **MUSTARD** was traffic stopped for running a red light. **MUSTARD** also denied having any involvement in any fraudulent gas purchase scheme. She additionally claimed to have no knowledge of any of the suspects involved in the scheme. It was later learned that **MUSTARD** was observed appearing in video surveillance speaking with the suspects who were determined to be involved in the fraud scheme.

46. The store employee advised that he recognized the second suspect who was wearing the black warm up suit from a prior October 16, 2019 encounter when he had entered the store asking for a "blunt wrapper."

47. A review of **MUSTARD's Facebook** page by law enforcement officials resulted in the possible identification of the two male suspects connected to the said Sammy's Gas Station incident. **MUSTARD's Facebook** page confirmed that she routinely communicates with

a man named **DAVID MONROE**. A number of posted *Facebook* photos of **MONROE** depict him wearing the same said Chicago Bears football jersey bearing #34. The second male suspect was determined by law enforcement authorities to be **TYSON THOMAS**.

48. During the evening hours of October 27, 2019, DPD Officers were dispatched to 307 South Woodward Avenue in response to a “shots fired” complaint. Upon arriving on-scene, Officers spoke to the complainant Danielle Dudley. She reported hearing five (5) gunshots followed shortly thereafter by approximately 10 more shots all in rapid succession. Dudley indicated that she believed the shots originated from a residence located at 218 South Kilmer Street.

49. Officers thereafter approached 218 South Kilmer Street where they observed parked in the driveway, a newer model Black Infiniti Q50 automobile with pitch black window tint bearing registration plate GYM8190. Officers also observed several (Tulammo) 7.62 x 39 caliber shell casings laying in the driveway. Officers knocked on the door of said residence whereupon **TYSON THOMAS** responded wearing a haircut cape around his upper torso. He indicated he was in the process of getting a haircut. Officers advised **THOMAS** that they have found several shell casings in his driveway and inquired whether he knew who may have been involved in shooting firearms. **THOMAS** turned back towards the house and shouted “Hey Uncle, these officers want to know about those guys that were shooting in the alley!” After a few moments, another black male, later identified to be **PATRICK PATTERSON** appeared from the back of the residence. He indicated he didn’t know who was shooting firearms on his property, and told us to “come back with a warrant.” **PATTERSON** thereafter refused to speak with the Officers about the shooting.

50. The Officers returned thereafter to their cruisers and ran the license plate on the said Black Infiniti Q50. Officers determined that the license plate returned to a 1991 Black Chevrolet registered to a Bria Crawford. At that point, the Officers returned back to the 218



South Kilmer Street residence to find that the Black Infiniti Q50 had since been moved. Officers determined that the vehicle had been relocated to the backyard of residence located across the street at 217 South Kilmer Street. The now unoccupied vehicle appeared to have been driven over a number of concrete blocks prior to coming to its present parked location. The Officers approached the parked and unoccupied vehicle. The Officers ran a LEADS inquiry of the VIN number and learned the vehicle had been reported as stolen out of Butler County Sheriff's Office. The Officers at that point returned to 218 South Kilmer residence in search **THOMAS** and **PATTERSON**. Neither individual was to be found. The Officers thereafter returned back to the stolen vehicle to report the situation via Teletype. As the Officers began processing the stolen vehicle, **THOMAS** unexpectedly appeared from the North side of 217 S. Kilmer and walked towards the front bumper of the Infiniti Q50. He was observed to be carrying a paper sack which contained an unknown object. He was then observed talking on a cellphone. Due to the dark lighting conditions, **THOMAS** was unaware that the Officers were standing next to the vehicle. Upon discovering the presence of the Officers, **THOMAS** immediately turned and fled on foot. Officers gave chase through the backyard area of 210 S. Kilmer St. where **THOMAS** attempted to jump a fence. Despite the Officers' repeated commands for **THOMAS** to stop, he ignored these orders and jumped said fence. Eventually **THOMAS** was subdued after **THOMAS** had discarded the paper sack. **THOMAS** was detained in handcuffs and escorted to the back seat of a DPD cruiser. The discarded paper sack was subsequently recovered adjacent to a Draco AK-74 rifle, and a loaded P-Magazine which contained identical ammunition previously observed on the driveway of 218 S. Kilmer. Two of **THOMAS**' cell phones were also located near the said fence, to wit: a RED IPHONE WITH RED CASE, hereinafter referred to as Device #6; and a SILVER IPHONE WITH BLACK CASE AND RED COVER IMEI: 354387064785382, MODEL: A1522, FCC ID: BCG-E2817A, hereinafter referred to as Device #7, Borth cell phones were recovered by law enforcement at this time.

51. **THOMAS** was detained in the back seat of a police cruiser. While in that location, he made several spontaneous utterances, to include: “Man, I didn’t know that car was stolen. When you guys get into the car can you grab my bag for me? My iPad is in it.” It should be noted that the Officers had never advised **THOMAS** that the Infiniti Q50 was known to be stolen. **THOMAS** also stated that he wanted his back pack from the vehicle and both of his red phones. **THOMAS** indicted that that Bria Crawford was his wife.

52. The stolen vehicle was impounded, inventory searched and towed. A back pack was found on the passenger seat. Located inside of the back pack were: a BLACK AND SILVER IPAD, MODEL: A2200, SERIAL # GG7ZCGG0MDG1, (hereinafter referred to as Device #8), along with the Tulammo 7.62x39 ammunition identical to that found inside of the Draco AK-74 and in the driveway of 218 S. Kilmer Street. Officers also located a clear Ziploc baggie containing several bags of marijuana and a scale. Officers additionally found inside the back pack several .45 caliber Winchester rounds and a black container which contained a credit card scanning device, and approximately 50 gift cards.

53. The Officers performed a CCH search through Teletype. This search revealed that **THOMAS** had previously been convicted in 2016 of Having a Weapon While Under Disability in Montgomery Common Pleas Court, in Case # 2016-cr-02368.

54. **TYSON THOMAS** was thereafter transported to the DPD Public Safety Building for an interview. After being advised of his 5<sup>th</sup> Amendment *Miranda* warnings, **THOMAS** agreed to answer questions.

55. **THOMAS** advised law enforcement that his cell phones had assigned numbers of 937-242-3552 and 937-673-1763 (smaller iPhone). **THOMAS** refused to provide law enforcement with the passcodes for the phones, and the required thumbprint required for his iPad. **THOMAS** stated that he had several gift cards because he was trying to figure out how to put money on the gift cards by manipulating the track data. **THOMAS** indicated he first learned

about the re-encoding scam from a person he only identified as “FAT KEV”, “FAT ASS” and “BIG DUDE” that he claimed to have previously met at a gas station. “FAT KEV” explained to **THOMAS** that he has an unlimited number of gas station gift cards and could fill up his tank for \$20. “FAT KEV” further explained that **THOMAS** could fill up gas for both his girlfriend’s and mom’s cars if he bought some cards off of him. He ultimately agreed to do so for \$4 each.

56. **THOMAS** stated that the first batch of cards he purchased from “FAT KEV” did not work because the gas pumps required zip code verification. **THOMAS** advised “FAT KEV” that the cards didn’t work. “FAT KEV” in-turn advised **THOMAS** to purchase more cards which he agreed to do. These new cards also did not work. At that point, “FAT KEV” told **THOMAS** to buy a card reader, writer, and encoder so that he could check his own cards. **THOMAS** stated that he paid “FAT KEV” \$80 per card to have two cards with chips embedded and encoded with credit card numbers.

57. Det. Dulaney inquired of **THOMAS** as to whether “FAT KEV” was in fact **KEVIN ALEXANDER** who lives directly across the street from him on Rockcliff Circle. **THOMAS** responded he doesn’t mess with anyone on his street. Det. Dulaney told **THOMAS** that it appeared rather peculiar that he had gift cards encoded with credit card numbers and intended to use those cards at gas stations which was the exact same *modus operandi* known to have been used by **KEVIN ALEXANDER**. **THOMAS** stated he doesn’t mess with **KEVIN ALEXANDER** because “he is being watched by the feds.”

58. A total of 45 credit cards were found on **TYSON THOMAS**’ person. Out of these 45 cards, 14 had credit card numbers encoded.



### **TECHNICAL TERMS**

59. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated

“GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.



- i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

60. Based on my prior training, experience, and research, I know that each of the seized electronic devices have the potential capability to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and/or a PDA. Based on my prior training and experience, examining data stored on devices of this type. It is possible to forensically uncover, among other things, evidence that reveals or suggests who possessed or used the device.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

61. Based on my knowledge, training, and experience, I know that certain electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

62. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw



conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

63. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant being applied for would permit authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

64. *Manner of execution.* Because this sought after warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto any premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### CONCLUSION

65. I submit that this affidavit establishes the necessary probable cause required for the issuance of search warrants authorizing the examination of the stored electronic data currently contained in each of the seized electronic devices (previously described as Devices #1, #2, #3, #4, #5, #6, #7, and #8) as described in Attachment A, for the specific listed items of information set forth in Attachment B.

**REQUEST FOR SEALING**

66. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

  
TREVOR CANFIELD  
Special Agent  
United States Secret Service

Subscribed and sworn to before me  
this 17th day of March, 2020.

  
SHARON L. OVINGTON  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

The property sought to be searched consists of: a WHITE IPHONE 10 hereinafter referred to as Device #1; an unknown version of an IPHONE (damaged) inside of BLACK CASE hereinafter referred to as Device #2; an ACER CHROME LAPTOP COMPUTER, Serial: NXGV2AA002927094067600, Model: N17Q8, SNID: 92703789476 hereinafter referred to as Device #3; a BLACK LG CELL PHONE WITH CRACKED SCREEN hereinafter referred to as Device #4; an IPHONE7 WITH BLACK CASE hereinafter referred to as Device #5; a RED IPHONE WITH RED CASE hereinafter referred to as Device #6; a SILVER IPHONE WITH BLACK CASE AND RED COVER IMEI: 354387064785382, MODEL: A1522, FCC ID: BCG-E2817A hereinafter referred to as Device #7; and a BLACK AND SILVER IPAD, MODEL: A2200, SERIAL # GG7ZCGG0MDG1 hereinafter referred to as Device #8.

All said Devices are presently stored and maintained in a secure evidence locker maintained at the U.S. Secret Service Offices located at 200 West Second St., Ste. #811, Dayton, OH 45402. They remain in the same state and condition as when they were first transferred into the USSS' custody from the various local law enforcement agencies who originally seized them.

This warrant seeks authorization to forensically examine of each of the said Devices for the purpose of identifying the electronically stored information described in Attachment B.



**ATTACHMENT B**

1. All records stored on the aforesaid Devices #1, #2, #3, #4, #5, #6, #7 and #8, as described in Attachment A that relate to possible violations of Title 18, United States Code, §§ 1028, 1028A, 1029, 1030, 1343, 1344, 371, and 1349. These suspected offenses specifically involve, or may involve the actions of various known and unknown individuals who have engaged a fraudulent and criminal conspiracy to illicitly credit/debit and gift cards to steal gas from local Dayton, Ohio gas stations dating back to at least on or about January 1, 2018, including:
  - a. Names, lists of addresses, telephone nos. and e-mail addresses of all possible conspirators and “customers” of said fraud conspiracy;
  - b. Names, lists of addresses, dates, telephone no. and e-mail addresses associated with all possible victim retail gas stations;
  - c. Types, amounts, dates, locations and prices charged for any and all illicit gas fill-up events;
  - d. Dates, places, and locations of specific fraudulent transactions;
  - e. Any and all information relating to the sources and individuals from which the conspiracy obtained suspected stolen credit card account numbers, to include “Dark Web” sources;
  - f. Any and all possible sources and origins of stolen credit card account numbers, and/or plastic credit/gift and/or debit cards;
  - g. Any and all information concerning any travel schedule or arrangements of conspirators and other whereabouts dating from January 1, 2018 until the present;
  - h. Any and all information concerning any associated conspirators or associates’ bank records, checks, credit card bills, debit card bills, gift card accounts, and any other associated account information, and other financial records.
2. Evidence of user attribution showing who used or owned the said Devices between the time period of January 1, 2018 until present.
3. Any and all records evidencing the use or access of the so-called Internet, “Dark Web” and *Facebook* including:
  - i. records of any Internet Protocol addresses used;

- ii. records of any Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- iii. records of any “Dark Web” activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

**ATTACHMENT C**

18 U.S.C. § 1028	Fraud and Related Activity in Connection Identification Documents, Authentication Features and Information
18 U.S.C. § 1028A	Aggravated Identity Theft
18 U.S.C. § 1029	Access Device Fraud
18 U.S.C. § 1030	Fraud and Related Activity in Connection with Computers
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1344	Bank Fraud
18 U.S.C. §§ 371 and 1349	Conspiracy to Commit an Offense Against the United States or Defraud the United States